

# Cyber Smart

## Get Familiar with Cyber Basics

At a time when we are more connected than ever, being “cyber smart” is of the utmost importance. This year has already seen more than a fair share of attacks and breaches, including the SolarWinds and Kaseya breaches as well as high-profile attacks on the Colonial Pipeline and other critical infrastructure. Furthermore, as has been underlined by these recent breaches, cyber attacks are becoming more sophisticated with more evolved bad actors cropping up each day. Luckily, there are several steps that we can take on a daily basis to mitigate risks and stay one step ahead of malefactors.

Here are a few quick tips:

### **Enable MFA**

Multi-factor authentication (MFA) adds that necessary second check to verify your identity when logging in to one of your accounts. By requiring multiple methods of authentication, your account is further protected from being compromised, even if a bad actor hijacks your password. In this way, MFAs make it more difficult for password cracking tools to enable attackers to break into accounts.

### **Use strong passphrases/password manager**

This may seem obvious, but all too often securing strong passphrases/password managers is overlooked. People spending more time online during the pandemic has certainly contributed to more bad actors prowling for accounts to attack. Using long, complex, and unique passwords is a good way to stop your account from being hacked, and an easy way of keeping track and remembering your passwords is by using a password manager.

### **Perform software updates**

When a device prompts that it's time to update the software, it may be tempting to simply click postpone, and ignore the message. However, having the latest security software, web browser, and operating system on devices is one of the best defenses against online threats. So, don't wait - update with the guidance and supervision of a trusted technology partner.

### **Do your research**

Common sense is a crucial part of maintaining good online hygiene, and an intuitive step to stay safe online is to do some research before downloading anything new you are downloading to your device, such as apps. Before downloading any new learning app on your device, make sure that it's a by checking who created the app, what the user reviews say, and if there are any articles published online about the app's privacy and security features.

### **Check your settings**

Be diligent to double check your privacy and security settings, and be aware who can access your documents. This extends from Google docs, to Zoom calls, and beyond. For meetings on Zoom, for example, create passwords so only those invited to the session can attend, and restrict who can share their screen or files with the rest of the attendees.

Phones/VoIP • Networks • PC Support • Secure Backup

970.242.8142 • [info@commwestcorp.com](mailto:info@commwestcorp.com)

[www.commwestcorp.com](http://www.commwestcorp.com)